REMARKS

I. Introduction

In response to the Office Action dated September 28, 2009, which was made final, and in conjunction with the Request for Continued Examination (RCE) submitted herewith, claims 1 and 16 have been amended. Claims 1-30 remain in the application. Re-examination and re-consideration of the application is requested.

II. Prior Art Rejections

A. The Office Action Rejections

In paragraph (4) of the Office Action, claims 1-7, 10-13, 16-22, and 25-28 were rejected under 35 U.S.C. §103(a) as being unpatentable over McDonnell et al., U.S. Patent No. 7,512,234 (McDonnell) in view of Kubo et al., U.S. Patent No. 7,007,168 (Kubo). In paragraph (16) of the Office Action, claims 14-15 and 29-30 were rejected under 35 U.S.C. §103(a) as being unpatentable over McDonnell in view of Kubo and further in view of Denning et al., U.S. Patent No. 7,143,289 (Denning). In paragraph (19) of the Office Action, claims 8-9 and 23-24 are rejected under 35 U.S.C. §103(a) as being unpatentable over McDonnell in view of Kubo and further in view of Clapper, U.S. Publication No. 2003/0108202 (Clapper).

Applicants' attorney respectfully traverses these rejections.

B. The Applicants' Independent Claims

Independent claims 1 and 16 are generally directed to the identification, processing, and comparison of location coordinate data in a confidential and anonymous manner. Independent claim 1 is representative and recites: receiving a plurality of fixed coordinates that represent a location of an item, the plurality of fixed coordinates being generated by more than one process; utilizing a cryptographic algorithm to encrypt the plurality of fixed coordinates, thereby forming a processed data; and comparing the encrypted fixed coordinates of the processed data to at least a portion of secondary data that comprises one or more encrypted fixed coordinates to determine whether a relationship exists between the encrypted fixed coordinates of the processed data and the encrypted fixed coordinates of the secondary data.

C. The McDonnell Reference

McDonnell describes how location data about a mobile entity is provided in encrypted form by a location server to a recipient that is one of the mobile entity or a service system usable by the mobile entity. The location data is encrypted such that it can only to be decrypted using a secret available to a decryption entity that is not under the control of the recipient. This permits location data to be provided in a confidential manner to service systems and also protects billing relationships between participants. A mechanism is also described for limiting the accuracy of decrypted location data made available to a service system.

D. The Kubo Reference

Kubo describes user authentication using member specifying discontinuous different coordinates. In an authentication apparatus, coordinates input from a coordinate detector via a plurality of discontinuous holes or openings, cutouts or marks provided on a member which is used to specify the coordinates are detected, and an authentication is made based on a comparison result of the detected coordinates and a plurality of registered coordinates.

E. The Denning Reference

Denning describes a system and method for delivering encrypted information in a communication network using location identity and key tables, wherein access to digital data is controlled by encrypting the data in such a manner that, in a single digital data acquisition step, it can be decrypted only at a specified location, within a specific time frame, and with a secret key. Data encrypted in such a manner is said to be geo-encrypted. This geo-encryption process comprises a method in which plaintext data is first encrypted using a data encrypting key that is generated at the time of encryption. The data encrypting key is then encrypted (or locked) using a key encrypting key and information derived from the location of the intended receiver. The encrypted data encrypting key is then transmitted to the receiver along with the ciphertext data. The receiver both must be at the correct location and must have a copy of the corresponding key decrypting key in order to derive the location information and decrypt the data encrypting key. After the data encrypting key is decrypted (or unlocked), it is used to decrypt the ciphertext. If an attempt is made to decrypt the data encrypting key at an incorrect location or using an incorrect secret key, the decryption will fail. If the sender so elects, access to digital data also can be

controlled by encrypting it in such a manner that it must traverse a specific route from the sender to the recipient in order to enable decryption of the data. Key management can be handled using either private-key or public-key cryptography. If private-key cryptography is used, the sender can manage the secret key decrypting keys required for decryption in a secure manner that is transparent to the recipient. As a consequence of its ability to manipulate the secret keys, the sender of encrypted data retains the ability to control access to its plaintext even after its initial transmission.

F. The Clapper Reference

Clapper describes location dependent encryption and/or decryption, wherein encryption and decryption may be tied to physical location information, e.g., GPS or other position data. Decryption keys may be defined with respect to a location at which decryption is to occur. A clock may be used to ensure decryption is occurring at a desired decryption location. For security, names may be associated with GPS position data, where encrypted data and a name associated with position data may be provided to a recipient, and the recipient is required to know or have access to the position data associated with the name in order to compute a decryption key. For additional security, encryption may also be performed with respect to position data for an encryption location, where an identifier associated with the encryption location is provided to the recipient, and the recipient is required to know or have access to the position data associated with the second name. Other embodiments are disclosed.

G. The Applicants' Invention is Patentable Over the References

The Applicants' claimed invention is patentable over the references, because the claims contain limitations not taught by the reference. Specifically, Applicants' invention is designed to use a cryptographic algorithm to identify, disclose and compare multiple sets of coordinates representing the location of a particular item in a secure and confidential manner. These essential features are not taught or suggested by the references.

The Office Action, on the other hand, asserts the following:

> Claims 1-7, 10-13, 16-22, and 25-28 are rejected under 35 U.S.C. 103 (a) as being unpatentable over McDonnell et al (hereinafter referred as McDonnell)

US 7,512,234 B2 in view of Kubo et al (hereinafter referred as Kubo) US Patent No 7,007168 B2.

As per claims 1, 16: McDonnell discloses a method/computer readable medium for identification processing and comparison of location coordinate data in a confidential and anonymous manner comprising: receiving, in a computer, a plurality of fixed coordinates, represents a location of an item more than one process (See col. 9 lines 44-47 (i.e., obtain location data)); utilizing, in the computer, a cryptographic algorithm to process the plurality of fixed coordinates forming a processed data (See col. 6 lines 49-56 and col. 9 lines 56-60 (i.e., encrypt location data)).

McDonnell does not explicitly teach comparing, in the computer, the encrypted fixed coordinates of the processed data to at least a portion of secondary data that comprises one or more encrypted fixed coordinates to determine whether a relationship exists between the encrypted fixed coordinates of the processed data and the encrypted fixed coordinates of the secondary data.

However Kubo teaches comparing the encrypted fixed coordinates of the processed data to at least a portion of secondary data that comprises one or more encrypted fixed coordinates to determine whether a match exists between the encrypted fixed coordinates of the processed data and the encrypted fixed coordinates of the secondary data (See col. 10 lines 18-27, col. 16 lines 39-67 and Figs 18A, Fig 23 steps S 193-195)

Therefore it would have been obvious to one ordinary skill in the art at that time the invention was made to employ the teachings method of Kubo within Denning method in order to provide delivering encrypted information in a communication network using location data.

Applicants' attorney disagrees, and submits that the combination of McDonnell and Kubo fails to teach or suggest all the limitations of Applicants' claims.

Specifically, McDonnell does not teach or suggest the elements of the independent claims directed to "comparing the encrypted fixed coordinates of the processed data to at least a portion of secondary data that comprises one or more encrypted fixed coordinates to determine whether a relationship exists between the encrypted fixed coordinates of the processed data and the encrypted fixed coordinates of the secondary data."

Consider, for example, the portions of McDonnell cited by the Office Action, which are set forth below:

McDonnell: col. 6, lines 49-56 (actually, lines 46-56)

According to the present invention, there is provided a method of providing location data about a mobile entity, wherein the location data is provided in encrypted form by a location server to a recipient that is one of the mobile entity or a service system usable by the mobile entity, the location data being encrypted such that it can only to be decrypted using a secret available to a

decryption entity that is not under the control of the recipient, whereby involvement of the decryption entity is necessary to decrypt the location data.

McDonnell: col. 9, lines 44-47

[I]f the location data is in the form of X, Y coordinates, then the aforesaid components are X and Y coordinate components of the mobile entity's location.

McDonnell: col. 9, lines 56-60

The mobile entity 20 also uses the encrypted location data in package P to request (arrow 75) a second location aware service from a second service system 40A, this time with a higher accuracy limit specified in package Q.sub.2.

Consider also other pertinent portions of McDonnell, which are set forth below:

McDonnell: col. 8, line 44 – col. 9, line 4

The mobile entity 20 now supplies (arrow 72) the encrypted location data to a first service system 40A with a request for a first location-aware service; because of privacy concerns, the user of the mobile entity does not want the service system to know his/her location with a high degree of accuracy and accordingly specifies an accuracy limit as a quality of service parameter in data package Q.sub.1. Package Q.sub.1 also includes the identity of the service system 40A and the period of validity of the request (for example, 10 minutes). Packages P and Q.sub.1 are together digitally signed by mobile entity 20 using the private key of the user (the digital signature S is shown in FIG. 7 as enclosing the packages P and Q.sub.1 within a dotted box). As a result, the encrypted location data and the parameters contained in package Q.sub.1 cannot be altered or substituted without this being detectable.

Before the service system 40A can act upon the request from mobile entity 20, it must have the location data L decrypted by decryption entity 80; the decryption entity is such that it will not decrypt the location data unless also provided with package Q.sub.1 protected by digital signature S--this is done so that the decryption entity can reliably limit the accuracy of the location data it returns to the level specified by the mobile entity. Accordingly, service system 40A next passes the digitally-signed packages P and Q.sub.1 (arrow 73) to the entity 80; for security reasons, the connection between the service system 40A and decryption entity 80 is preferably an encrypted connection with authentication of the participating parties (for example, an SSL or TLS connection).

McDonnell: col. 9, lines 48-51

Step 86--**The decrypted location data L.sub.1 with accuracy limited to the level specified by the QoS parameter set by the mobile entity is then returned to the service system 40A over the secure link** (arrow 74 in FIG. 7).

The above portions of McDonnell merely describe how location data for a mobile entity remains encrypted until a decryption entity decrypts it for use by a service system. However,

nowhere do the above portions of McDonnell describe a comparison being performed between encrypted coordinate data.

Indeed, the Office Action admits that McDonnell does not explicitly teach "comparing the encrypted fixed coordinates of the processed data to at least a portion of secondary data that comprises one or more encrypted fixed coordinates to determine whether a relationship exists between the encrypted fixed coordinates of the processed data and the encrypted fixed coordinates of the secondary data."

Nonetheless, the Office Action asserts that Kubo shows these elements of the independent claims at the following locations:

Kubo: Fig. 18A

FIG. 18A

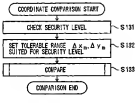


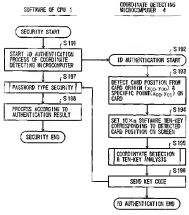
FIG. 18B

SECURITY LEVEL	TOLERABLE RANGE
1	$(\Delta x_1, \Delta y_1)$
⋮	⋮
m	$(\Delta x_m, \Delta y_m)$
⋮	⋮
t	$(\Delta x_t, \Delta y_t)$

HERE $\Delta x_1 > \cdots > \Delta x_m > \cdots > \Delta x_t$
$\Delta y_1 > \cdots > \Delta y_m > \cdots > \Delta y_t$

Kubo: Fig. 23

FIG. 23



Kubo: col. 10, lines 18-27

When starting the computer system shown in FIG. 1, the user ID is input and the ID authentication is made according to the present invention after the BIOS is loaded and before the operating system is loaded. Further, the user ID is input and the ID authentication is made according to the present invention when starting the application. **Compared to the conventional user ID input which is made by inputting text data which is made up of numbers, alphabets and the like, the present invention inputs the user ID by inputting coordinate values unique to the user. The present invention makes the authentication of the user ID by judging whether or not the input coordinate values or a coordinate value pattern is correct, so as to improve the security of the computer system. The user ID input and the ID authentication will now be described in more detail.**

Kubo: col. 16, lines 39-67

In FIG. 11, a step S91 sets on the screen 11 a 10.times.n software ten-key corresponding to the size of the card. More particularly, the software ten-key is made up of n rows of 10 keys "0" through "9" shown in FIG. 12B which will be described later, and this software ten-key is set at the origin (x0, y0) which is determined by the random number on the screen 11 shown in FIG. 12A.

A step S92 calculates comparison coordinates from the position coordinates of the software ten-key and the registered data. As described above, the origin (x0, y0) is added to the position coordinates of the software

ten-key to calculate the coordinates on the screen 11 as the comparison coordinates.

A step S93 displays only the card frame, and the software ten-key itself is not displayed on the screen 11.

A step S101 notifies an input coordinate to the software of the CPU 1 if an input is made on the screen 11.

A step S102 decides whether or not the input exists. If the decision result in the step S102 is YES, a step S103 detects the input coordinate, and a step S104 notifies the input coordinate to the software of the CPU 1.

A step S94 makes a coordinate check and a ten-key analysis. More particularly, a check is made to determine the coordinate of the ten-key corresponding to the input coordinate notified in the step S104, and the coordinate of the ten-key is converted into a corresponding key of the ten-key.

A step S95 carries out a so-called password type security by discriminating whether or not the key converted from the coordinate of the ten-key in the step S104 matches the registered data with respect to the column of the numerical values (0, 1, 2, . . . , 9) of the keys of the ten-key.

The above portions of Kubo merely describe authenticating a user by inputting coordinate values unique to the user to generate a key code comprising a user ID, and then authenticating the user ID by determining whether the coordinate values are correct. This technique of Kubo is considered more secure than the user merely entering a conventional user ID as text data.

For example, Kubo uses a 10 x n software ten-key corresponding to the size of the card, wherein the software ten-key is made up of n rows of 10 keys "0" through "9" as shown in FIG. 12B. The card position coordinates determine which of the keys in the software ten-key are selected and output as the user ID data, which is then compared to the registered user ID data, in order to authenticate the user.

While the card position coordinates in Kubo are used to generate a key code as the user ID, the coordinates are never used in encrypted form. Further, because the card position coordinates in Kubo are never encrypted, they are never compared with other encrypted location information to determine whether a relationship exists. Moreover, the resulting key code in Kubo itself is never encrypted or compared with another (e.g., registered) encrypted version of the key code.

Consequently, the combination of McDonnell and Kubo does not teach or suggest the limitations of Applicants' independent claims directed to "comparing the encrypted fixed coordinates of the processed data to at least a portion of secondary data that comprises one or

more encrypted fixed coordinates to determine whether a relationship exists between the encrypted fixed coordinates of the processed data and the encrypted fixed coordinates of the secondary data."

Indeed, neither McDonnell nor Kubo operate in the same context as Applicants' claims, namely using a cryptographic algorithm to identify, process and compare sets of encrypted coordinates in a secure and confidential manner. Instead, McDonnell operates in the context of delivering encrypted location information that can be decrypted only by a specified decryption entity, while Kubo operates in the context of user authentication using input coordinates to generate a key code as the basis for the authentication.

Moreover, the Denning and Clapper references do not overcome the deficiencies of the Denning reference. Recall that Denning was cited only against dependent claims 14-15 and 29-30 and only for disclosing a plurality of fixed coordinates represent a location, and Clapper was cited only against dependent claims 8-9 and 23-24 and only for disclosing a uniform and non-uniform grid, in the context of overlaying a residential area.

Thus, Applicants' attorney submits that independent claims 1 and 16 are allowable over McDonnell, Kubo, Denning and Clapper. Further, dependent claims 2-15 and 17-30 are submitted to be allowable over McDonnell, Kubo, Denning and Clapper in the same manner, because they are dependent on independent claims 1, and 16, respectively, and thus contain all the limitations of the independent claims. In addition, dependent claims 2-15 and 17-30 recite additional novel elements not shown by Denning, Kubo, Denning and Clapper.

III. Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Please consider this a PETITION FOR EXTENSION OF TIME for a sufficient number of months to enter these papers, if appropriate. Please charge all fees to Deposit Account No. 09-0460 of IBM Corporation, the assignee of the present application.

Respectfully submitted,

GATES & COOPER LLP
Attorneys for Applicants

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, California 90045
(310) 641-8797

Date: December 28, 2009

By: /George H. Gates/
Name: George H. Gates
Reg. No.: 33,500

GHG/

G&C 30571.303-US-U1